

(2) 39

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-187101

(43)Date of publication of application : 04.07.2003

(51)Int.Cl.

G06F 17/60

H04L 9/32

H04N 7/167

H04N 7/173

(21)Application number : 2001-385453 (71)Applicant : SONY CORP

(22)Date of filing : 19.12.2001 (72)Inventor : CHIN KOGUN

### (54) INFORMATION PROCESSORINFORMATION PROCESSING METHODSTORAGE MEDIUMINFORMATION PROCESSING SYSTEM AND PROGRAM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To protect a copyright of a content when making content transferable by peer-to-peer.

**SOLUTION:** Transmission and receipt of encrypted content data between a content server 4 and a personal computer 1-1 is executed without using public key cryptosystem as shown by (a) in a Figure. User information containing information ID showing the source of the content data is described in a field attached to the content data as shown by b in the Figure. Since the user information is encrypted by the public key of a license server 3only the license server 3 can read it. Electronically signed preview license acquisition request information or general license acquisition request information is transmitted to the license server 3 as shown by c in the Figure. The information showing the source of the content data is described in the license acquisition request information as shown by d in the Figure.

### CLAIMS

[Claim(s)]

[Claim 1]An information processor comprising:

An acquisition means which acquires contents.

A creating means which generates the 4th information including the 1st information attached to said contents,the 2nd information for specifying said contentsand the 3rd

information that can specify itself.

The 1st transmitting means that transmits said 4th information generated by said creating means.

A reception means which receives the 5th information required in order to reproduce said contentsAn extraction means to extract the 6th information attached to said 5th information received by said reception meansand an information attachment means to make said 6th information extracted by said extraction means attach to said contents instead of said 1st information attached to said contents.

[Claim 2]The information processor according to claim 1 having further the 2nd transmitting means that transmits said contents to which said 6th information was attached by said information attachment means to other information processors.

[Claim 3]The information processor according to claim 1wherein said 1st information and said 6th information are enciphered by a public key of a transmission destination of said 4th information.

[Claim 4]The information processor according to claim 1wherein said 5th information is the 2nd either 1st license information for reproducing said contents by conditioning or license information for reproducing said contents thoroughly.

[Claim 5]The information processor according to claim 1 having further an encoding means which enciphers said 4th information generated by said creating means.

[Claim 6]The information processor according to claim 5 said encoding means's enciphering said 4th information by a public key of a transmission destination of said 4th informationand performing an electronic signature with its own secret key.

[Claim 7]The information processor according to claim 1 having further a decoding means which decodes said 5th information received by said reception means.

[Claim 8]An acquisition control step which controls acquisition of contentsand the 1st information attached to said contentsA generation step which generates the 4th information including the 2nd information for specifying said contentsand the 3rd information that can specify itselfA transmission-control step which controls transmission of said 4th information generated by processing of said generation stepA reception-control step which controls reception of the 5th information required in order to reproduce said contentsAn extraction step which extracts the 6th information attached to said 5th information by which reception was controlled by processing of said reception-control stepAn information processing method containing an information attachment step which makes said 6th information extracted by processing of said extraction step attach to said contents instead of said 1st information attached to said contents.

[Claim 9]An acquisition control step which controls acquisition of contentsand the 1st information attached to said contentsA generation step which generates the 4th information including the 2nd information for specifying said contentsand the 3rd information that can specify itselfA transmission-control step which controls

transmission of said 4th information generated by processing of said generation stepA reception-control step which controls reception of the 5th information required in order to reproduce said contentsAn extraction step which extracts the 6th information attached to said 5th information by which reception was controlled by processing of said reception-control stepA recording medium with which a program which a computer containing an information attachment step which makes said 6th information extracted by processing of said extraction step attach to said contents instead of said 1st information attached to said contents can read is recorded.

[Claim 10]An acquisition control step which controls acquisition of contentsand the 1st information attached to said contentsA generation step which generates the 4th information including the 2nd information for specifying said contentsand the 3rd information that can specify itselfA transmission-control step which controls transmission of said 4th information generated by processing of said generation stepA reception-control step which controls reception of the 5th information required in order to reproduce said contentsAn extraction step which extracts the 6th information attached to said 5th information by which reception was controlled by processing of said reception-control stepA program making a computer perform processing containing an information attachment step which makes said 6th information extracted by processing of said extraction step attach to said contents instead of said 1st information attached to said contents.

[Claim 11]An information processor comprising:

An acquisition means which acquires contents.

A creating means which generates the 4th information including the 1st information attached to said contentsthe 2nd information for specifying said contentsand the 3rd information that can specify itself.

A transmitting means which transmits said 4th information generated by said creating means.

A reception means which receives the 5th information required in order to reproduce said contentsAn information attachment means to make said 6th information enciphered by an encoding means which enciphers the 6th information that can specify itself by a public key of a transmission destination of said 4th informationand said encoding means attach to said contents instead of said 1st information attached to said contents.

[Claim 12]An information processing method comprising:

An acquisition control step which controls acquisition of contents.

A generation step which generates the 4th information including the 1st information attached to said contentsthe 2nd information for specifying said contentsand the 3rd information that can specify itself.

A transmission-control step which controls transmission of said 4th information generated by processing of said generation step.

A reception-control step which controls reception of the 5th information required in order to reproduce said contents  
An encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of said 4th information  
An information attachment step which makes said 6th information enciphered by processing of said encryption step attach to said contents instead of said 1st information attached to said contents.

[Claim 13]An acquisition control step which controls acquisition of contentsand the 1st information attached to said contents  
A generation step which generates the 4th information including the 2nd information for specifying said contentsand the 3rd information that can specify itself  
A transmission-control step which controls transmission of said 4th information generated by processing of said generation step  
A reception-control step which controls reception of the 5th information required in order to reproduce said contents  
An encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of said 4th information  
A recording medium with which a program which a computer containing an information attachment step which makes said 6th information enciphered by processing of said encryption step attach to said contents instead of said 1st information attached to said contents can read is recorded.

[Claim 14]An acquisition control step which controls acquisition of contentsand the 1st information attached to said contents  
A generation step which generates the 4th information including the 2nd information for specifying said contentsand the 3rd information that can specify itself  
A transmission-control step which controls transmission of said 4th information generated by processing of said generation step  
A reception-control step which controls reception of the 5th information required in order to reproduce said contents  
An encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of said 4th information  
A program making a computer perform processing containing an information attachment step which makes said 6th information enciphered by processing of said encryption step attach to said contents instead of said 1st information attached to said contents.

[Claim 15]An information processor comprising:

The 1st recording device that records the 1st information peculiar to said contents that it is used in order to reproduce contents.

A reception means which receives the 5th information that includes the 2nd information attached to said contents  
the 3rd information for specifying said contentsand the 4th information for specifying an information processor besides the above from other information processors which hold said contents.

An extraction means to extract said 1st information corresponding to said contents specified using said 3rd information among said 1st information currently recorded on said 1st recording device.

The 1st creating means that generates the 6th information that includes at least information which specifies an information processor besides the aboveThe 2nd creating means that generates the 7th information that includes at least said 6th information generated by said 1st creating means and said 1st information extracted by said extraction meansA transmitting means which transmits said 7th information generated by said 2nd creating means to an information processor besides the above specified using said 4th information.

[Claim 16]Have further an encoding means which enciphers said 6th information generated by said 1st creating means by its own public keyand said 2nd creating meansThe information processor according to claim 15 generating the 7th information that includes at least said 6th information enciphered by said encoding means and said 1st information extracted by said extraction means.

[Claim 17]The information processor according to claim 15 which is further provided with a decoding means which decodes said 2nd information included in said 5th information received by said reception means using its own secret keyand is characterized by said 2nd information being information enciphered by said public key.

[Claim 18]The information processor according to claim 15wherein said 1st information is the 2nd either 1st license information for reproducing said contents by conditioning or license information for reproducing said contents thoroughly.

[Claim 19]The information processor according to claim 15 having further an encoding means which enciphers said 7th information generated by said 2nd creating means.

[Claim 20]The information processor according to claim 19 said encoding means's enciphering said 7th information by a public key of an information processor besides the above specified using said 4th informationand performing an electronic signature with its own secret key.

[Claim 21]The information processor according to claim 15 having further a decoding means which decodes said 5th information received by said reception means.

[Claim 22]The 2nd recording device that is included in said 5th information received by said reception means and that records said 2nd informationsaid 3rd informationand said 4th informationThe information processor according to claim 15 having further an analysis means to analyze information about said contentsbased on said 2nd information recorded by said 2nd recording devicesaid 3rd informationand said 4th information.

[Claim 23]A record control step which controls record of the 1st information peculiar to said contents used in order to reproduce contentsThe 2nd information attached to said contents from other information processors which hold said contentsA reception-control step which controls reception of the 5th information including the 3rd information for specifying said contentsand the 4th information for specifying an information processor besides the aboveAn extraction step which extracts said 1st information corresponding to said contents specified using said 3rd information among

said 1st information by which record is controlled by processing of said record control stepThe 1st generation step that generates the 6th information that includes at least information which specifies an information processor besides the aboveThe 2nd generation step that generates the 7th information that includes at least said 6th information generated by processing of said 1st generation stepand said 1st information extracted by processing of said extraction stepAn information processing method containing a transmission-control step which controls transmission to an information processor besides the above specified using said 4th information on said 7th information generated by processing of said 2nd generation step.

[Claim 24]A recording medium with which a program which a computer can read is recordedcomprising:

A record control step which controls record of the 1st information peculiar to said contents used in order to reproduce contents.

A reception-control step which controls reception of the 5th information including the 2nd information attached to said contents from other information processors which hold said contentsthe 3rd information for specifying said contentsand the 4th information for specifying an information processor besides the above.

An extraction step which extracts said 1st information corresponding to said contents specified using said 3rd information among said 1st information by which record is controlled by processing of said record control step.

The 1st generation step that generates the 6th information that includes at least information which specifies an information processor besides the aboveThe 2nd generation step that generates the 7th information that includes at least said 6th information generated by processing of said 1st generation stepand said 1st information extracted by processing of said extraction stepA transmission-control step which controls transmission to an information processor besides the above specified using said 4th information on said 7th information generated by processing of said 2nd generation step.

[Claim 25]A program making a computer perform processing characterized by comprising the following.

A record control step which controls record of the 1st information peculiar to said contents used in order to reproduce contents.

A reception-control step which controls reception of the 5th information including the 2nd information attached to said contents from other information processors which hold said contentsthe 3rd information for specifying said contentsand the 4th information for specifying an information processor besides the above.

An extraction step which extracts said 1st information corresponding to said contents specified using said 3rd information among said 1st information by which record is controlled by processing of said record control step.

The 1st generation step that generates the 6th information that includes at least

information which specifies an information processor besides the aboveThe 2nd generation step that generates the 7th information that includes at least said 6th information generated by processing of said 1st generation stepand said 1st information extracted by processing of said extraction stepA transmission-control step which controls transmission to an information processor besides the above specified using said 4th information on said 7th information generated by processing of said 2nd generation step.

[Claim 26]An information processing system constituted by 1st at least one information processor characterized by comprising the following that acquires contents and is reproducedand the 2nd information processor that transmits information for reproducing said contents to said 1st information processor. An acquisition means from which said 1st information processor acquires said contents.

The 1st creating means that generates the 4th information including the 1st information attached to said contentsthe 2nd information for specifying said contentsand the 3rd information that can specify itself.

The 1st transmitting means that transmits said 4th information generated by said 1st creating means to said 2nd information processor.

The 1st reception means that receives the 5th information required in order to reproduce said contents transmitted from said 2nd information processor.

The 1st extraction means that extracts the 6th information attached to said 5th information received by said reception means.

Said 6th information extracted by said 1st extraction means is replaced with said 1st information attached to said contentsA recording device which records the 7th information peculiar to said contents that it is used in order to have an information attachment means made to attach to said contents and for said 2nd information processor to reproduce said contents.

The 2nd reception means that receives said 1st informationsaid 2nd informationand said 4th information including said 3rd information from said 1st information processorThe 2nd extraction means that extracts said 7th information corresponding to said contents specified using said 2nd information among said 7th information currently recorded on said recording deviceThe 2nd creating means that generates said 6th information that includes at least information which specifies said 1st information processorThe 3rd creating means that generates said 5th information that includes at least said 6th information generated by said 2nd creating means and said 7th information extracted by said 2nd extraction meansThe 2nd transmitting means that transmits said 5th information generated by said 3rd creating means to said 1st information processor specified using said 3rd information.

## DETAILED DESCRIPTION

---

### [Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is an information processor and an information processing method, a recording medium, an information processing system, and it is used when it provides the contents distribution service. It is peer-to-peer and contents can be delivered and received about a program by the users which receive service especially, and it is related with a suitable information processor and information processing method, a recording medium, an information processing system, and a program.

[0002]

[Description of the Prior Art] The users who record composition data, picture image data, etc. on the inside of a personal computer, and he reincarnates and enjoys themselves are increasing in number with improvement in the increase in the storage capacity of a personal computer and the reproduction art of a sound or an image.

[0003] What is called contents data of composition data, picture image data, etc. is downloadable via the Internet, etc. from the website which the entrepreneur who is performing the contents distribution service manages. It is also possible for it to be peer-to-peer and to deliver and receive contents between personal computers.

[0004]

[Problem(s) to be Solved by the Invention] However, when it is peer-to-peer and delivers and receives contents between the personal computers which a user holds, it is dramatically difficult to keep the copyright of contents. Therefore, it considers distributing the contents data enciphered with the decode key to an authorized user (for example, user who paid the fee).

[0005] Contents data is enciphered, and if the user who was peer-to-peer and received contents data is prevented from viewing and listening to contents data, it becomes impossible, however, to circulate contents widely using peer to peer one.

[0006] Before a user pays a fee in order that the contents data may confirm whether it is what suited its taste, for example, if it is music data, will try listening and think that he would like to check the contents of contents data. Therefore, the contents distribution service entrepreneur needs to distribute the data for an audition of contents data [for example] (some, etc.) to which it can view and listen apart from the enciphered contents data, for example, without using a decode key.

[0007] This invention being made in view of such a situation, enabling the audition of contents to a user before the purchase of contents data and keeping the copyright of contents. It enables it to circulate contents widely and enables it to carry out tracing of the flow of contents further using peer to peer one.

[0008]

[Means for Solving the Problem] Since an acquisition means which acquires



contents the 1st information attached to contents and contents are specified this invention is characterized by the 1st information processor comprising the following.  
A creating means which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

The 1st transmitting means that transmits the 4th information generated by creating means.

A reception means which receives the 5th information required in order to reproduce contents.

An extraction means to extract the 6th information attached to the 5th information received by a reception means and an information attachment means to make the 6th information extracted by an extraction means attach to contents instead of the 1st information attached to contents.

[0009] It can have further the 2nd transmitting means that transmits contents to which the 6th information was attached by an information attachment means to other information processors.

[0010] The 1st information and the 6th information shall be enciphered by a public key of a transmission destination of the 4th information.

[0011] The 5th information shall be the 2nd either 1st license information for reproducing contents by conditioning or license information for reproducing contents thoroughly.

[0012] It can have further an encoding means which enciphers the 4th information generated by creating means.

[0013] An encoding means is made to encipher the 4th information by a public key of a transmission destination of the 4th information and an electronic signature can be made to perform to it with its own secret key.

[0014] A decoding means which decodes the 5th information received by a reception means can be made to have further.

[0015] Since an acquisition control step which controls acquisition of contents and the 1st information and contents which are attached to contents are specified this invention is characterized by the 1st information processing method comprising the following.

A generation step which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

A transmission-control step which controls transmission of the 4th information generated by processing of a generation step.

A reception-control step which controls reception of the 5th information required in order to reproduce contents.

An extraction step which extracts the 6th information attached to the 5th information by which reception was controlled by processing of a reception-control step and an information attachment step which makes the 6th information extracted by processing

of an extraction step attach to contents instead of the 1st information attached to contents.

[0016] Since an acquisition control step which controls acquisition of contents and the 1st information and contents which are attached to contents are specified, this invention is characterized by a program currently recorded on the 1st recording medium comprising the following.

A generation step which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

A transmission-control step which controls transmission of the 4th information generated by processing of a generation step.

A reception-control step which controls reception of the 5th information required in order to reproduce contents.

An extraction step which extracts the 6th information attached to the 5th information by which reception was controlled by processing of a reception-control step and an information attachment step which makes the 6th information extracted by processing of an extraction step attach to contents instead of the 1st information attached to contents.

[0017] An acquisition control step by which the 1st program of this invention controls acquisition of contents. A generation step which generates the 4th information including the 1st information attached to contents, the 2nd information for specifying contents, and the 3rd information that can specify itself. A transmission-control step which controls transmission of the 4th information generated by processing of a generation step. A reception-control step which controls reception of the 5th information required in order to reproduce contents. An extraction step which extracts the 6th information attached to the 5th information by which reception was controlled by processing of a reception-control step. A computer is made to perform processing containing an information attachment step which makes the 6th information extracted by processing of an extraction step attach to contents instead of the 1st information attached to contents.

[0018] Since an acquisition means which acquires contents, the 1st information attached to contents, and contents are specified, this invention is characterized by the 2nd information processor comprising the following.

A creating means which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

A transmitting means which transmits the 4th information generated by creating means.

A reception means which receives the 5th information required in order to reproduce contents.

An information attachment means to make the 6th information enciphered by an

encoding means which enciphers the 6th information that can specify itself by a public key of a transmission destination of the 4th information and encoding means attach to contents instead of the 1st information attached to contents.

[0019] Since an acquisition control step which controls acquisition of contents and the 1st information and contents which are attached to contents are specified, this invention is characterized by the 2nd information processing method comprising the following.

A generation step which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

A transmission-control step which controls transmission of the 4th information generated by processing of a generation step.

A reception-control step which controls reception of the 5th information required in order to reproduce contents.

An encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of the 4th information and an information attachment step which makes the 6th information enciphered by processing of an encryption step attach to contents instead of the 1st information attached to contents.

[0020] Since an acquisition control step which controls acquisition of contents and the 1st information and contents which are attached to contents are specified, this invention is characterized by a program currently recorded on the 2nd recording medium comprising the following.

A generation step which generates the 4th information including the 2nd information and the 3rd information that can specify itself.

A transmission-control step which controls transmission of the 4th information generated by processing of a generation step.

A reception-control step which controls reception of the 5th information required in order to reproduce contents.

An encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of the 4th information and an information attachment step which makes the 6th information enciphered by processing of an encryption step attach to contents instead of the 1st information attached to contents.

[0021] An acquisition control step by which the 2nd program of this invention controls acquisition of contents. A generation step which generates the 4th information including the 1st information attached to contents, the 2nd information for specifying contents, and the 3rd information that can specify itself. A transmission-control step which controls transmission of the 4th information generated by processing of a

generation stepA reception-control step which controls reception of the 5th information required in order to reproduce contentsAn encryption step which enciphers the 6th information that can specify itself by a public key of a transmission destination of the 4th informationA computer is made to perform processing containing an information attachment step which makes the 6th information enciphered by processing of an encryption step attach to contents instead of the 1st information attached to contents.

[0022]The 1st recording device that records the 1st information peculiar to contents that it is used in order for this invention to reproduce contentsSince the 2nd information and contents which are attached to contents are specified from other information processors which hold contentsit is characterized by the 3rd information processor comprising the following.

A reception means which receives the 3rd information and the 5th information including the 4th information for specifying other information processors.

An extraction means to extract the 1st information corresponding to contents specified using the 3rd information among the 1st information currently recorded on the 1st recording device.

The 1st creating means that generates the 6th information that includes at least information which specifies other information processors.

The 2nd creating means that generates the 7th information that includes at least the 6th information generated by the 1st creating means and the 1st information extracted by an extraction meansand a transmitting means which transmits the 7th information generated by the 2nd creating means to other information processors specified using the 4th information.

[0023]Can have further an encoding means which enciphers the 6th information generated by the 1st creating means by its own public keyand to the 2nd creating means. The 7th information that includes at least the 6th information enciphered by encoding means and the 1st information extracted by an extraction means can be made to generate.

[0024]A decoding means which decodes the 2nd information included in the 5th information received by a reception means using its own secret key shall be made to have furtherand the 2nd information shall be information enciphered by public key.

[0025]The 1st information shall be the 2nd either 1st license information for reproducing contents by conditioning or license information for reproducing contents thoroughly.

[0026]An encoding means which enciphers the 7th information generated by the 2nd creating means can be made to have further.

[0027]An encoding means is made to encipher the 7th information by a public key of other information processors specified using the 4th informationand an electronic signature can be made to perform with its own secret key.

[0028]A decoding means which decodes the 5th information received by a reception means can be made to have further.

[0029]The 2nd recording device that records the 2nd informationthe 3rd informationand the 4th information which are included in the 5th information received by a reception meansAn analysis means to analyze information about contents can be made to have further based on the 2nd informationthe 3rd informationand the 4th information which were recorded by the 2nd recording device.

[0030]A record control step which controls record of the 1st information peculiar to contents used in order for this invention to reproduce contentsSince the 2nd information and contents which are attached to contents from other information processors which hold contents are specifiedit is characterized by the 3rd information processing method comprising the following.

A reception-control step which controls reception of the 5th information including the 3rd information and the 4th information for specifying other information processors.

An extraction step which extracts the 1st information corresponding to contents specified using the 3rd information among the 1st information by which record is controlled by processing of a record control step.

The 1st generation step that generates the 6th information that includes at least information which specifies other information processors.

The 2nd generation step that generates the 7th information that includes at least the 6th information generated by processing of the 1st generation stepand the 1st information extracted by processing of an extraction stepA transmission-control step which controls transmission to other information processors specified using the 4th information on the 7th information generated by processing of the 2nd generation step.

[0031]A record control step which controls record of the 1st information peculiar to contents used in order for this invention to reproduce contentsSince the 2nd information and contents which are attached to contents from other information processors which hold contents are specifiedit is characterized by a program currently recorded on the 3rd recording medium comprising the following.

A reception-control step which controls reception of the 5th information including the 3rd information and the 4th information for specifying other information processors.

An extraction step which extracts the 1st information corresponding to contents specified using the 3rd information among the 1st information by which record is controlled by processing of a record control step.

The 1st generation step that generates the 6th information that includes at least information which specifies other information processors.

The 2nd generation step that generates the 7th information that includes at least the 6th information generated by processing of the 1st generation stepand the 1st information extracted by processing of an extraction stepA transmission-control step

which controls transmission to other information processors specified using the 4th information on the 7th information generated by processing of the 2nd generation step.

[0032]A record control step which controls record of the 1st information peculiar to contents used in order for the 3rd program of this invention to reproduce contentsThe 2nd information attached to contents from other information processors which hold contentsA reception-control step which controls reception of the 5th information including the 3rd information for specifying contentsand the 4th information for specifying other information processorsAn extraction step which extracts the 1st information corresponding to contents specified using the 3rd information among the 1st information by which record is controlled by processing of a record control stepThe 1st generation step that generates the 6th information that includes at least information which specifies other information processorsThe 2nd generation step that generates the 7th information that includes at least the 6th information generated by processing of the 1st generation stepand the 1st information extracted by processing of an extraction stepA computer is made to perform processing containing a transmission-control step which controls transmission to other information processors specified using the 4th information on the 7th information generated by processing of the 2nd generation step.

[0033]An acquisition means from whichas for an information processing system of this inventionthe 1st information processor acquires contentsThe 1st creating means that generates the 4th information including the 1st information attached to contents,the 2nd information for specifying contentsand the 3rd information that can specify itselfThe 1st transmitting means that transmits the 4th information generated by the 1st creating means to the 2nd information processorThe 1st reception means that receives the 5th information required in order to reproduce contents transmitted from the 2nd information processorThe 1st extraction means that extracts the 6th information attached to the 5th information received by a reception meansThe 6th information extracted by the 1st extraction means is replaced with the 1st information attached to contentsA recording device which records the 7th information peculiar to contents that have an information attachment means made to attach to contentsand the 2nd information processor is used in order to reproduce contentsInside of the 7th information currently recorded on the 2nd reception means that receives the 1st informationthe 2nd informationand the 4th information including the 3rd information from the 1st information processorand a recording deviceThe 2nd extraction means that extracts the 7th information corresponding to contents specified using the 2nd informationThe 2nd creating means that generates the 6th information that includes at least information which specifies the 1st information processorThe 3rd creating means that generates the 5th information that includes at least the 6th information generated by the 2nd creating means and the 7th

information extracted by the 2nd extraction meansIt has the 2nd transmitting means that transmits the 5th information generated by the 3rd creating means to the 1st information processor specified using the 3rd information.

[0034]In the 1st information processor of this inventionan information processing methodand a programThe 1st information that contents are acquired and is attached to contentsthe 2nd information for specifying contentsAnd the 4th information including the 3rd information that can specify itself is generatedThe 4th generated information is transmittedthe 5th information required in order to reproduce contents is receivedthe 6th information attached to the 5th information is extractedand the 6th extracted information is attached to contents instead of the 1st information attached to contents.

[0035]In the 2nd information processor of this inventionan information processing methodand a programThe 1st information that contents are acquired and is attached to contentsthe 2nd information for specifying contentsAnd the 4th information including the 3rd information that can specify itself is generatedThe 5th information required in order to transmit the 4th generated information and to reproduce contents is receivedThe 6th information that can specify itself is enciphered by a public key of a transmission destination of the 4th informationand the 6th enciphered information is attached to contents instead of the 1st information attached to contents.

[0036]In the 3rd information processor of this inventionan information processing methodand a programThe 1st information peculiar to contents that it is used in order to reproduce contents is recordedThe 2nd information attached to contents from other information processors which hold contentsThe 5th information including the 3rd information for specifying contents and the 4th information for specifying other information processors is receivedThe 1st information corresponding to contents specified using the 3rd information among the 1st information currently recorded is extractedThe 7th information that the 6th information that includes at least information which specifies other information processors is generatedand includes the 6th generated information and the 1st extracted information at least is generatedand the 7th generated information is transmitted to other information processors specified using the 4th information.

[0037]In an information processing system of this inventionare the 1st information processor and contents are acquiredThe 1st information attached to contentsthe 2nd information for specifying contentsAnd the 4th information including the 3rd information that can specify itself is generatedThe 5th information required in order to reproduce contents which the 4th generated information was transmitted to the 2nd information processorand were transmitted from the 2nd information processor is receivedInstead of the 1st information attached to contentsthe 6th information attached to the 5th information is extractedit is attached to contents by the 6th extracted informationand with the 2nd information processor. The 7th information peculiar to contents that it is used in order to reproduce contents is recordedFrom

the 1st information processor the 1st information the 2nd information and the 4th information including the 3rd information are received The 7th information corresponding to contents specified using the 2nd information among the 7th information currently recorded is extracted The 5th information that the 6th information that includes at least information which specifies the 1st information processor is generated and includes the 6th generated information and the 7th extracted information at least is generated The 5th generated information is transmitted to the 1st information processor specified using the 3rd information.  
[0038]

[Embodiment of the Invention] Hereafter an embodiment of the invention is described with reference to figures.

[0039] Drawing 1 is a network composition figure used in order to provide the contents distribution service which was adapted in this invention.

[0040] The personal computer 1-1 thru/or 1-n which a user holds is connected with the license server 3 the contents server 4 and the settling server 5 via the Internet 2.

[0041] The personal computer 1-1 thru/or 1-n receive contents from the contents server 4 via the Internet 2 (download). There is a thing of various gestalten such as picture image data based on composition data image data still picture information dynamic image data or dynamic image data and voice data in contents data for example.

[0042] The contents server 4 searches the contents data for which the user using the personal computer 1-1 thru/or 1-n asks from the contents database 13 and transmits to the personal computer 1-1 thru/or 1-n via the Internet 2. The contents data currently recorded on the contents database 13 is enciphered. It may be made for the contents server 4 to exhibit the website (download site) which can download contents for example on the Internet 2.

[0043] The contents management table registered into the contents database 13 with contents data is explained using drawing 2.

[0044] License ID etc. which are used when reproducing the content ID which is peculiar ID showing contents the address information which shows the place which is recording contents and corresponding contents are recorded on the contents management table. As for license ID license ID for a license and license ID for a preview license are usually registered. Since the contents server 4 does not publish a license and the contents database 13 does not necessarily save the license over contents either it is not necessary to necessarily register license ID in a contents management table. However the decode key (license key) for decoding the contents contained in a license It is more desirable to manage the relation between license ID and content ID in the contents management tables since the contents servers 4 are the enciphering key which enciphered each contents and a key which accomplishes a couple.

[0045] A license is usually a license which can reproduce contents thoroughly here and



a preview license is a license which can perform what is called trial reproduction (for example reproduction of some contents etc.) for checking a part of the contents.

[0046] With personal computers 1-1 other than oneself thru/or personal computer 1-n the personal computer 1-1 thru/or personal computer 1-n can be peer-to-peer and can transmit and receive the contents data received from the contents server 4. It cannot be overemphasized that the contents data received from other personal computers can be transmitted to other personal computers that it is peer-to-peer and similarly.

[0047] Thus it is enciphered and cannot reproduce view and listen to the circulating contents data only by receiving contents data. Then the personal computer 1-1 thru/or 1-n require transmission of the license for reproducing contents data to the license server 3 via the Internet 2.

[0048] In order for the personal computer 1-1 thru/or 1-n to receive a license from the license server 3 it is necessary to perform user registration by processing mentioned later beforehand. The license server 3 receives the input of user registration information from the personal computer 1-1 thru/or 1-n and publishes user ID which is a number peculiar to each of a user which is registered.

[0049] The user registration database 11 and the license information database 12 are connected to the license server 3. Or a user is distributed from the contents server 4 using the personal computer 1-1 thru/or 1-n it is peer-to-peer and he publishes the license for reproducing the contents copied from other personal computers.

[0050] The usual license which can decode all the contents data with a license there is a preview license which can reproduce the contents (what is called -- degradation was carried out) on which a part of restrictive reproduction i.e. contents for a user to check the contents of contents or the bit rate and resolution were dropped. The personal computer 1-1 thru/or 1-n usually require a license or a preview license of a license server.

[0051] The license status which shows a license whether it is usually a license or it is a preview license. The decode key (license key) for decoding predetermined contents and if needed. User Information used in order to carry out tracing of the limitation information which shows the restrictions in the case of reproducing copy guard information and contents (for example a refreshable period the number of times of refreshable or the number of times which can be copied etc.) and the distribution channel of contents is included. In order to show the distribution origin of contents in User Information the information which can specify a user is included at least and user ID etc. are enciphered by the public key of the license server 3 for example. It may be made to include the variety of information etc. which accompany contents also besides mentioning above in a license.

[0052] The settling server 5 usually performs accounting of the user who holds the personal computer 1-1 thru/or 1-n and the administrator of the license server 3 in advance of license issue. It may be made for the settlement of accounts using the

credit card transaction and the prepaid card for example as a charging method the settlement of accounts by electronic money etc. to use which method.

[0053] It distributes from the contents server 4 and the field for indicating User Information is added to contents data peer-to-peer and received [ between the personal computer 1-1 thru/or 1-n / deliver and ].

[0054] For example from the contents server 4 when contents are distributed User Information of the contents server 4 including the information which shows that it distributed from the contents server 4 is indicated in the field. And when the license of corresponding contents is (even a preview usually) acquired with the personal computer 1-1 which the user A holds with a license. User Information including the information for specifying the user A is included and the information indicated in the field is rewritten by the user's A User Information.

[0055] And when the contents are peer-to-peer and are transmitted to the personal computer 1-2 which the user B holds from the personal computer 1-1 which the user A holds User Information of the user of the user A who becomes the distribution origin of contents is indicated in the field. And in the personal computer 1-2 which the user B holds when a license is acquired the user's B User Information is included in the license and the information indicated in the field attached to contents is rewritten by the user's B User Information.

[0056] In this system in order that the license server 3 the registered personal computer 1-1 or 1-n may deliver and receive the information that safety is high via the Internet 2 a public-key crypto system shall be used. Therefore the license server 3 transmits to the personal computer 1-1 thru/or 1-n which the user who had the public key of a license server registered uses while obtaining a user's public key registered at the time of user registration.

[0057] A public-key crypto system is one of the data encryption methods. In a public-key crypto system keys (bit string) different respectively are used by a data transmission person's data encryption and decoding of a data receiving person's data (by a private key crypto system the same key is used on the both sides of encryption and decoding to a public-key crypto system).

[0058] In a public-key crypto system two kinds of keys a "public key" and a "secret key" are used. Among these the user who generated it keeps the secret key in the safe place and no is opened to others. One public key is widely distributed to the partner (data may be sent to itself) who may become transmitting [ data ] origin. Specifically it may attach to an E-mail may send to a partner it deposits with the entrepreneur who offers service which manages a public key and anyone may enable it to refer to it. And the sending person of data obtains the public key which the reception destination publishes is a public key of a reception destination and enciphers the data to transmit. In this way in order to decode the enciphered data the secret key corresponding to the public key used for encryption is required. For this reason data cannot be decoded even if a third party without a secret key monitors data.

[0059]In order to generate the key pair of a "public key" and a "secret key"there are some methodsbut the RSA algorithm advocated by RivestShamirand Adleman is famous. In RSAa public key and a secret key are generated using the product of a huge number of prime numbers which amount to hundreds of figures. In order to have generated while from such a prime number and to draw another side from a valuefactorization into prime factors of a huge number is needed. Huge computation is required for factorization into prime factors of this huge numberand it is impossible to take out an answer to within a time [ realistic ]. Herean RSA algorithm may be used for generation of a key pairor other methods may be used.

[0060]The "secret key" in a public-key crypto system can be used also as an "electronic signature" the addresser of the data proves it to be that he is the person himself/herself rightly. As mentioned aboveby the usual encryptiondata is enciphered by the public key which the reception destination publishedbut in an electronic signatureit enciphers with its own secret keyand the data (value which usually applied hash to data) which a sending agency transmits is made into an electronic signatureis added to dataand is sent to a partner. The partner who received this decodes an electronic signature using the public key which the transmitting origin published. And the received data (hash value of data) is compared with the data which decoded the electronic signatureif in agreementit will be the information which the person himself/herself disseminated rightlyand not being altered will be proved. Herethe data which enciphered data by the public key of the reception destinationand performed the electronic signature with the secret key for the electronic signatures of a transmitting agency shall be transmitted and received.

[0061]Howeverin the public-key crypto systemit must be illuminated whether the public key really belongs to the person himself/herself. thenan independent organization -- public -- the person himself/herself -- PKI (Public Key Infrastructure) for attesting is used.

[0062]In PKIa certificate authority which is called a certificate authority (CA:Certification Authority) and which can trust it is provideda public key is published and managed with the "electronic certificate" by an electronic signatureand the mechanism of proving the justification (it is the person himself/herself) of the transfer place of data is provided. Therebytapping and an alterationor spoofing of data can be prevented.

[0063]The personal computer 1-1 thru/or 1-n which the license server 3 and a registered user hold exchanges a mutual public key. And it is enciphered and the license server 3 receives the signed license acquisition request information from either the personal computer 1-1 which a registered user holds or thru/or the 1-n. User Information indicated in a transmission source user's (license request origin) user IDthe content ID of the contents which require acquisition of a licenseand the field incidental to the contents is attached to license acquisition request information.

[0064]The license server 3 which received license acquisition request informationA

license table is referred to from the license information database 12. Search the license key (decode key to contents) corresponding to content ID for example user ID etc. generate User Information including the information for specifying a license supply destination. It enciphers by the public key of a license server license status information limitation information etc. are added and a license is generated. After the license server 3 enciphers a license and performs an electronic signature it transmits to transmitting [ license acquisition request information ] origin via the Internet 2. A license table is mentioned later.

[0065] And the license server 3 on the license issue table of the license information database 12. Record the history of license issue and the information (tracing information is called hereafter) which shows via what kind of user contents data is circulating is extracted based on the information attached to license acquisition request information. It records on the tracing information table of the license information database 12. A license issue table and a tracing information table are mentioned later.

[0066] Hereafter when the personal computer 1-1 thru/or personal computer 1-n do not need to be distinguished separately it is only named the personal computer 1 generically.

[0067] Drawing 3 is a block diagram showing the composition of the personal computer 1.

[0068] CPU (Central Processing Unit) 21 Via the signal corresponding to the various instructions which the user inputted via I/O interface 22 and the internal bus 23 using the input part 24 and the network interface 30. For example various processing based on the inputted signal is performed in response to the input of the signal which the license server 3 etc. transmitted. ROM (Read Only Memory) 25 stores fixed data fundamentally of the parameters the program which CPU 21 uses and for an operation. In the program used in execution of CPU 21 and its execution RAM (Random Access Memory) 26 stores a variable parameter suitably. CPU 21 ROM 25 and RAM 26 are mutually connected by the internal bus 23.

[0069] The internal bus 23 is connected also with I/O interface 22. The input part 24 consists of a keyboard a touch pad a jog dial or a mouse and when a user inputs various kinds of instructions into CPU 21 it is operated for example. . The outputting part 27 comprises CRT (Cathode Ray Tube) a liquid crystal display etc. for example. It comprises an indicator which displays a variety of information in a text or an image a loudspeaker for which a sound is outputted a buzzer which generates a sound further if needed a LED lamp for transmitting information to a user by lighting or putting out light etc.

[0070] HDD (hard disk drive) 28 drives a hard disk and records or reproduces the program and information (for example contents data) which are performed by CPU 21 to them. The drive 29 is equipped with the magnetic disk 31 the optical disc 32 the magneto-optical disc 33 and the semiconductor memory 34 if needed and data is

delivered and received to it.

[0071]The Internet 2 is accessed and the network interface 30 performs transfer of the license server 3 etc. and information via the Internet 2. The network interface 30 may be connected with the memory storage of the exterior which has memorized contents data for example.

[0072]These input parts 24 thru/or network interfaces 30 is connected to CPU 21 via I/O interface 22 and the internal bus 23.

[0073]Fundamentally since it has the same composition as the personal computer 1 the license server 3 thru/or the settling server 5 also omit the detailed explanation about the hardware.

[0074]Drawing 4 is a functional block diagram showing the function of the license server 3 which publishes the usual license for reproducing the contents data which performs user registration of the user using the personal computer 1 and the personal computer 1 is recording or a preview license.

[0075]The control section 41 controls operation of the license server 3 based on the variety of information which was inputted via the Internet 2 and I/O interface 42 and which was transmitted from the personal computer 1. The control section 41 registers into the user registration database 11 a user's registration information etc. which were transmitted from the personal computer 1 for example or. Are recorded on the personal computer 1 which the newly registered user holds by the memory 43. A public key contents decoding application program etc. of the license server 3 are transmitted or the license of corresponding contents is generated in response to a license acquisition request and the processing which transmits to the personal computer 1 of a requiring agency is controlled.

[0076]I/O interface 42 is an interface for the license server 3 to perform transfer of the user registration database 11 the license information database 12 and the Internet 2 and information.

[0077]The public key of the license server 3 the information transmitted to the personal computers 1 such as a contents decoding application program and a variety of information required for processing of the control section 41 are recorded on the memory 43.

[0078]In communication with the personal computer 1 which a registered user has encryption and the decoding processing section 44 encipher the information to transmit and while they sign the signature of the received information is checked the processing which decodes and User Information attached to a license are enciphered or processing which decodes User Information included in license acquisition request information is performed. Encryption and the decoding processing section 44 save the secret key of the license server 3 which equips the inside with the secret key Records Department 51 and is used for the check of encryption and a signature.

[0079]The tracing data analysis part 45 based on User Information etc. which are

attached to license acquisition request information. Each contents analyze in what kind of course it distributed to the user and extract useful various data from the data registered into the tracing information table of the license information database 12 in a contents distribution enterprise based on an analysis result.

[0080] Next with reference to the flow chart of drawing 5 processing with the personal computer 1 at the time of user registration execution and the license server 3 is explained.

[0081] In Step S1 CPU21 of the personal computer 1 According to the signal which shows a user's operation in which it was inputted from the input part 24 via I/O interface 22 and the internal bus 23 The license server 3 is accessed via the internal bus 23 I/O interface 22 the network interface 30 and the Internet 2. CPU21 of the personal computer 1 starts a web browser and it may be made to access the web page which the license server 3 exhibits for example.

[0082] In Step S2 CPU21 of the personal computer 1 transmits the public key (the object for data encryption and for signature decoding) of user registration information and a user to the license server 3. When exhibiting a public key generally it may be made to transmit the information about the obtaining method of a public key to the license server 3 here for example although the user's public key was explained as what transmits to the license server 3.

[0083] In Step S3 the control section 41 of the license server 3 Via the Internet 2 and I/O interface 42 the public key (or information about the obtaining method of a public key) of user registration information and a user is received and the user ID for the user who newly registers is set up.

[0084] In step S4 the control section 41 of the license server 3 registers the public key of user registration information and a user into the user registration database 11 via I/O interface 42 with the set-up user ID.

[0085] The user registration management table shown in drawing 6 is registered into the user registration database 11. In a user registration management table for every user ID which the license server 3 published. For example in addition to the mail address registered as the public key of the user for delivering and receiving information using the public-key crypto system mentioned above and a transmission destination of a license a user's personal information (a user's taste information etc. are included) etc. are registered if needed.

[0086] In Step S5 the control section 41 of the license server 3 reads a contents decoding application program from the memory 43 and transmits to the personal computer 1 via I/O interface 42 and the Internet 2. With a contents decoding application program. In the personal computer 1 generate and transmit license acquisition request information or At the time of license acquisition rewriting processing of User Information indicated in the field incidental to contents is performed or it is the application which performs processing decoded with the license which acquired contents data and the details are mentioned later.

[0087]In Step S6CPU21 of the personal computer 1 receives and installs a contents decoding application program. NamelyCPU21 records a contents decoding application program on HDD28and changes it into the state where it loads to RAM26 and can perform according to control of CPU21.

[0088]In Step S7the control section 41 of the license server 3The user ID set up in the public key (the object for data encryption and for signature decoding) of the license server 3 and Step S3 is transmitted to the personal computer 1 via I/O interface 42 and the Internet 2.

[0089]In Step S8CPU21 of the personal computer 1 receives the public key of a license serverand user IDrecords them on HDD28and processing ends it.

[0090]To a registered userthe user ID which is a peculiar number is set up for every userand it is recorded in both the license server 3 and the personal computer 1 by the registration processing explained above. And in order to deliver and receive the information by a public-key crypto systemthe license server 3While saving its own secret keyopen a public key to a registered user (it transmits to the personal computer 1 which a registered user has)and a registered userWhile saving a secret key in the personal computer 1 which he hasa public key is opened to the license server 3.

[0091]Although the license server 3 explains in drawing 5 as what sets up user IDFor exampleif those ID is individually assigned to the userit will not matter even if it diverts the user ID of other services already provided for the userapparatus ID currently individually assigned to apparatussuch as a portable telephone setetc.

[0092]Drawing 7 is a functional block diagram of the personal computer 1 when it receives at Step S6 of drawing 5 and the installed contents decoding application program has started.

[0093]The control section 61 controls operation of a contents decoding application program according to the operational input which the user performed using the input part 24. The control section 61 the license acquisition request information as which it was enciphered by encryption and processing of the decoding processing section 64and the electronic signature was indicated to befor example via I/O interface 62 and the Internet 2It transmits to the license server 3or the contents data received from the contents server 4 is saved at the contents database 66and the processing which updates the contents management table 67 is controlled.

[0094]I/O interface 62 is an interface for the personal computer 1 to perform transfer of the license server 3 thru/or the settling server 5and information via the Internet 2.

[0095]The memory 63 corresponds to HDD28ROM25or RAM26. The variety of information required for processing of the control section 61 is recorded on the memory 63 with the user ID published at the time of the public key of the license server 3 recorded in Step S8 of drawing 5and registrationand the personal information which is needed for accounting.

[0096]Encryption and the decoding processing section 64 encipher the information

transmitted in communication with the license server 3 check the signature of the received information and perform processing to decode and processing which decodes contents data using the license distributed from the license server 3 while they sign. Encryption and the decoding processing section 64 save a user's secret key which equips the inside with the secret key Records Department 71 and is used for the check of encryption and a signature.

[0097] The regeneration part 65 receives the contents entry of data decoded by encryption and the decoding processing section 64. According to a predetermined format required processing of data decompression processing error correction processing various Image Processing Division or D/A conversion processing of voice data is performed image data is outputted to the indicator 72 of the outputting part 27 and voice data is outputted to the loudspeaker 73 of the outputting part 27 respectively.

[0098] The contents database 66 is recording the enciphered contents data which was downloaded from the contents server 4. The content ID of the contents downloaded in the contents management table 67. The license key contained in the license received from the license server 3 with the contents management table later mentioned using the address information on which contents are recorded and drawing 11 which is recording the existence and license ID of a license is saved.

[0099] Next in the personal computer 1 which the registered user holds with reference to the flow chart of drawing 8 and drawing 9 The contents decoding application program explained using drawing 7 is loaded to RAM 26 and the processing in the case of performing in CPU 21 is explained.

[0100] While the control section 61 downloads desired contents and saves them from the contents server 4 via the Internet 2 and I/O interface 62 in Step S21 at the contents database 66. The information currently recorded on the contents management table 67 is updated. For example the control section 61 starts a web browser accesses the web page (download site) which the contents server 4 exhibits performs predetermined operation and it may be made to download desired contents data.

[0101] It is enciphered and contents cannot reproduce contents if there is no corresponding license even if it seems that data may be stolen by the malicious third party on a communication path. Therefore transmission and reception of the contents data of the contents server 4 and the personal computer 1-1 are performed without using the public-key crypto system mentioned above (inside a of the figure of drawing 10). In drawing 10 although the Internet 2 is not illustrated transfer of information is performed via the Internet 2.

[0102] As shown in [ of drawing 10 / b ] a figure in the field attached to the contents data downloaded from the contents server 4. User Information (information indicated to be con-server' among the figure) which shows that this contents data is the data downloaded from the contents server 4 is indicated. Since it is enciphered by the



public key of the license server 3 User Information is decoded only by encryption and the decoding processing section 44 of the license server 3.

[0103] User Information is enciphered by the public key of the license server 3 and it uses that reading is possible only in the license server 3. It is also possible to add the information which shows the time of the date of issue of a license and contents and the information about issue service of a license to User Information for example.

[0104] And the control section 61 manages the license corresponding to the enciphered contents data which downloads and is recorded on the contents database 66 and each contents using the contents management table 67.

[0105] The information registered into the contents management table 67 is explained using drawing 11. Within the content ID which is peculiar ID which expresses the contents saved at the contents database 66 to the contents management table 67 and the contents database 66 License ID usually for a license used when reproducing the address information which shows the place which is recording contents and corresponding contents and license ID for a preview license are registered. About the contents which have not performed issue requesting of the license yet of course license ID may not be registered but only license either one of license ID for a license or ID for a preview license may usually be registered depending on contents.

[0106] In Step S22 the control section 61 judges whether the input which orders it the license acquisition for preview reproduction was received from the user based on the signal which shows a user's operation in which it is inputted from the input part 24. In Step S22 when it is judged that the input which orders it the license acquisition for preview reproduction is not received processing progresses to Step S27.

[0107] When it is judged that the input which orders it the license acquisition for preview reproduction was received in Step S22 in Step S23 the control section 61 The preview license profitable demand information that the content ID of corresponding contents their own user ID and User Information (for example User Information including the information (con-server) which shows the contents server 4) added to the contents were attached is generated.

[0108] In Step S24 the control section 61 outputs the public key of the license server 3 currently recorded on the preview license acquisition request information generated in Step S23 and the memory 63 to encryption and the decoding processing section 64. Encryption and the decoding processing section 64 encipher preview license acquisition request information by the public key of the license server 3.

[0109] In Step S25 encryption and the decoding processing section 64 perform an electronic signature to preview license acquisition request information using the secret key for their signature currently recorded on the secret key Records Department 71.

[0110] In Step S26 the control section 61 transmits the preview license acquisition request information in which the electronic signature was enciphered and carried out by encryption and the decoding processing section 64 to the license server 3 via the

Internet 2 as shown in [ of drawing 10 / c ] a figure. In the preview license acquisition request information transmitted to the license server 3. User Information which shows that this contents data is the data downloaded from the contents server 4 as shown in [ of drawing 10 / d ] a figure (among a figure) The information indicated to be content server's own user ID (information indicated to be a1111111 among the figure) and content ID (information indicated to be xxxx among the figure) are indicated at least. [0111] The license server 3 judges here whether the conditions for preview license issue are fulfilled. A preview license is published when conditions are fulfilled (processing of Step S66 of drawing 15 and drawing 16 thru/or Step S68 mentioned later and Step S73 thru/or Step S76).

[0112] When it is judged that the input which orders it the license acquisition for preview reproduction is not received in Step S22, in Step S27 the control section 61 is judged whether based on the signal which shows a user's operation in which it is inputted from the input part 24 the input which orders it the license acquisition for ordinary reproduction was received from the user. In Step S27 when it is judged that the input which orders it the license acquisition for ordinary reproduction is not received, processing returns to Step S22 and processing after it is repeated.

[0113] When it is judged that the input which orders it the license acquisition for ordinary reproduction was received in Step S27, in Step S28 the control section 61 generates the usual license acquisition request information which attached the content ID of corresponding contents, its own user ID and User Information added to the contents is generated.

[0114] In Step S29 the control section 61 outputs the public key of the license server 3 which was generated in Step S28 and which is usually recorded on license acquisition request information and the memory 63 to encryption and the decoding processing section 64. Encryption and the decoding processing section 64 usually encipher license acquisition request information by the public key of the license server 3.

[0115] In Step S30 encryption and the decoding processing section 64 usually perform an electronic signature to license acquisition request information using the secret key for their signature currently recorded on the secret key Records Department 71.

[0116] The control section 61 is enciphered by encryption and the decoding processing section 64 in Step S31. Like the case which explained license acquisition request information in Step S26 where an electronic signature is carried out as shown in [ of drawing 10 / c ] a figure, it usually transmits to the license server 3 via the Internet 2. Like the case where it explains also to the preview license acquisition request information transmitted to the license server 3 in Step S26 as shown in [ of drawing 10 / d ] a figure, User Information which shows that this contents data is the data downloaded from the contents server 4 is indicated.

[0117] Here the license server 3 transmits the directions about accounting to the personal computer 1 and the settling server 5 (processing of Step S69 of drawing 16

mentioned later).

[0118]In Step S32the control section 61 receives the directions about accounting from the license server 5 via the Internet 2 and I/O interface 62as shown in [ of drawing 12 / e ] a figure. If neededit may be enciphered by a user's public keythe information which shows the directions about accounting here may be signed with the secret key of the license server 3 like the licenseand information may be made to be transmitted safely using other methods.

[0119]In Step S33after the control section 61 checks and decodes the signature of the received information by encryption and processing of the decoding processing section 64 if neededas shown in [ of drawing 12 / f ] a figureit accesses the settling server 5 and performs accounting according to the directions about accounting.

[0120]Herethe settling server 5 usually notifies the issue request of a license to the license server 3when accounting with a user is performed correctly. And the license server 3 usually publishes a licensewhen it judges including accounting whether the conditions for license issue are usually fulfilled and conditions are fulfilled (processing of Step S70 of drawing 16 thru/or Step S76 mentioned later).

[0121]In Step S34after the end of processing of Step S26or the end of processing of Step S33the control section 61As shown in [ of drawing 13 / h ] a figurethe data (namelylicense) which the electronic signature was carried out with the secret key for the signature of the license server 3and was enciphered by the user's public key is received from the license server 3 via the Internet 2 and I/O interface 62.

[0122]With a licenseas shown in [ of drawing 13 / g ] a figure. [ whether a license is usually a license and ] The license key for decoding the license status and contents which show whether it is a preview licensereproduction frequencylimitation informationsuch as regeneration timeand User Information enciphered by the public key of the license server are included. The informationincluding for examplethe user's user IDetc.which shows the licensed user is included in User Information included in the license.

[0123]Since this User Information is information peer-to-peer and received [ deliver and ] with contentsare enciphered by the public key of the license server so that the information which shows a third party a user may not be stolenbut. When User Information comprises only user IDfor examplethe enciphered data will be the same value each time. Thereforeby including other informationincluding the information about time and serviceetc.in User Informationfor example in addition to the information for specifying userssuch as user IDit is possible to prevent changing the value of enciphered User Information for every licenseand misusing User Information for a third party.

[0124]In Step S35encryption and the decoding processing section 64 check a signature using the public key for the signature of the license server 3 saved in the memory 63 to the received data.

[0125]In Step S36the control section 61 receives the result of the processing which

checks the signature which encryption and the decoding processing section 64 performed and judges whether transmitting [ the received data ] origin is the license server 3 rightly.

[0126]When it is judged that transmitting [ the received data ] origin is the license server 3 the control section 61 controls encryption and the decoding processing section 64 and makes the data which is a user's secret key currently recorded on the secret key Records Department 71 and was received decode in Step S37 in Step S36.

[0127]In Step S38 the control section 61 judges whether encryption and the decoding processing section 64 have decoded the received data correctly in Step S37.

[0128]transmitting [ the received data ] origin in Step S36 when it is judged that it is not the license server 3 In Step S38 when it is judged that the received data was not able to be decoded correctly in Step S39 the control section 61 displays an error message on the indicator 72 of the outputting part 27 and processing ends it.

[0129]When it is judged that the received data has been correctly decoded in Step S38 in Step S40 the control section 61 User Information included in the decoded license is extracted and in [ of drawing 13 / i ] a figure it rewrites with User Information of corresponding contents so that it may be shown (it overwrites). Therefore User Information indicated in the field attached to the contents license acquired turns into User Information including the information (for example user ID) which shows itself.

[0130]In Step S41 the control section 61 saves the decoded license (usually a license or a preview license) at the contents management table 67. And according to a user's operation in which the control section 61 is inputted from the input part 24 If needed contents are made to decode using the license key of the license saved at the contents management table 67 at encryption and the decoding processing section 64 the regeneration part 65 is controlled and the decoded contents are reproduced. Image data is outputted and displayed on the indicator 72 of the outputting part 27 among the reproduced contents and voice response of the voice data is outputted and carried out to the loudspeaker 27 of the outputting part 27.

[0131]Here the downloaded contents data is saved in the state where it was enciphered at the contents database 66. That is since the contents decoded by the license key are unrecordable a license key is used at every regeneration and decoding processing is performed. Thereby when restriction of reproduction frequency is included in the license regeneration of the unjust number of times can be prevented.

[0132]When the reproduction frequency of contents is restricted the user who reproduced the predetermined number of times usually demands a license of the license server 3 and newly reproduces corresponding contents. In this case of course since it is not necessary to re-download contents data as compared with the case where regulation of reproduction frequency is made and distributed to the contents data itself the user can lessen time to access the Internet 2 for download of contents data. And the contents distribution service entrepreneur can acquire just

remuneration to distribution of contents data by re-supply of a license preventing regeneration of the unjust number of times.

[0133]Next in Step S42 the control section 61 judges whether the peer to peer contents copy of data was required from other personal computers. For example the personal computer 1-1 of drawing 13 judges whether the copy of contents data was required from the registered personal computer 1-2 at the license server as shown in [ of drawing 13 / j ] a figure.

[0134]In [ when it is judged from other personal computers in Step S42 that the peer to peer contents copy of data was required ] Step S43 The control section 61 transmits the contents data in which User Information which shows itself was added to the personal computer of a requiring agency as shown in [ k ] a figure and processing is ended. In Step S42 when it is judged from other personal computers 1 that the peer to peer contents copy of data is not demanded processing is ended.

[0135]The personal computer 1-2 receives the contents data (contents data shown in [ of drawing 13 / i ] a figure) in which User Information of the personal computer 1-1 was added. Then as shown in [ of drawing 14 / l ] a figure the personal computer 1-2 The license acquisition request information to which content ID their own user ID and User Information of the personal computer 1-1 were added. It can encipher by the public key of the license server 3 it can sign with the secret key for a signature of the user who holds the personal computer 1-2 and can transmit to the license server 3 (inside m of the figure of drawing 14).

[0136]The license which the license server 3 performed predetermined processing mentioned above enciphered it by the public key of the user who holds the personal computer 1-2 and signed with the secret key for the signature of the license server 3 is transmitted to the personal computer 1-2 (inside n of the figure of drawing 14). As shown in [ o ] a figure User Information including license status a license key limitation information and the information including for example user ID etc. that shows the user who holds the personal computer 1-2 is included in this license. The personal computer 1-2 which received the license rewrites User Information indicated in the field added to the contents data saved for itself to its own User Information included in the received license (inside p of the figure of drawing 14).

[0137]The user using the personal computer 1 receives the settling server 5 Registration processing to the license server 3 explained using drawing 5 and same processing are performed it is made to perform registration processing and that it may be made to exchange the enciphered information has the settling server 5 and the natural personal computer 1.

[0138]In the processing explained using drawing 8 and drawing 9 Although the accounting performed with the settling server 5 and the personal computer 1 was explained in Step S33 as a thing to the license server 3 usually independently performed with transmission and reception of a license acquisition request or a license For example instead of usually transmitting license acquisition request

information to the license server 3 from the personal computer 1 the personal computer 1 Usually license acquisition request information is transmitted to the settling server 5 and it may be made for the settling server 5 to usually transmit license acquisition request information to the license server 3 after the end of accounting with the user ID of the user who performed accounting. In this case the license server 3 can be made into the thing which was transmitted from the settling server 5 and which is not usually received other than license acquisition request information.

[0139] Next with reference to drawing 15 and drawing 16 processing of the license server 3 performed in parallel to processing of the personal computer 1 explained using drawing 8 and drawing 9 is explained. Here the information for specifying a user included in User Information is explained as what is user ID.

[0140] In Step S61 the control section 41 of the license server 3 The data (data shown in [ of the inside c of the figure of drawing 10 or drawing 14 / m ] a figure) which the electronic signature was carried out with the secret key of the user who has the personal computer 1 and was enciphered by the public key of the license server 3 is received via the Internet 2 and I/O interface 42.

[0141] In Step S62 the control section 41 uses the address of the sending person of data etc. as a search key for example A user's public key registered into the user registration database 11 is searched it supplies with the data received in Step S61 to encryption and the decoding processing section 44 and an electronic signature is checked by the searched public key for a user's signature.

[0142] In Step S63 transmitting [ the data received based on whether the control section 41 has performed decoding processing in Step S62 ] origin judges whether it is a user's personal computer 1 registered.

[0143] In Step S63 when it is judged that transmitting [ the received data ] origin is not a user's personal computer 1 registered processing progresses to Step S78 mentioned later.

[0144] Transmitting [ the received data ] origin in Step S63 When it is judged that it is a user's personal computer 1 registered the control section 41 makes the received data decode in Step S64 using the secret key of the license server 3 currently recorded on encryption and the decoding processing section 44 by the secret key Records Department 51.

[0145] In Step S65 the control section 41 judges whether the received data decoded in Step S64 are preview license acquisition request information. In Step S65 when it is judged that received data are not preview license acquisition request information processing progresses to Step S69 mentioned later.

[0146] In Step S65 when it is judged that received data are preview license acquisition request information in Step S66 the control section 41 judges whether the conditions for preview license issue are fulfilled. For example the preview license acquisition request information by which the control section 41 was decoded. [ whether there is any inharmonious point in the contents of registration of the user registration

database 11 and ] (For example when you need the password whether the password is indicated accidentally.) When \*\*\*\* is checked or issue of the preview license is decided only once to be below the predetermined number of times by one contents With reference to the license information database 12 the issuance history of a preview license of a corresponding user is checked and it is checked whether it is a preview license request more than prescribed frequency.

[0147] In Step S66 when it is judged that the conditions for preview license issue are not fulfilled processing progresses to Step S78 mentioned later.

[0148] When it is judged in Step S66 that the conditions for preview license issue are fulfilled in Step S67 the control section 41 The content ID which requires a license based on the decoded preview license acquisition request information The license classification of license acquisition request information which received the user ID contained in User Information attached to license acquisition request information And the information about a license request including the user ID of license request origin etc. is registered into the tracing information table of the license information database 12.

[0149] A tracing information table is shown in drawing 17. The content ID attached to the tracing information table at license acquisition request information The license status which shows the classification of a license and the user ID contained in User Information i.e. the user ID of the distribution origin of contents and the distribution destination user ID which transmitted license acquisition request information are registered.

[0150] In Step S68 the control section 41 refers to the license table of the license information database 12 based on the content ID of which the preview license was required The license key for preview reproduction corresponding to the demanded contents is searched Generate User Information containing the user ID of the user who transmitted license acquisition request information at least and limitation informations such as regeneration time and the contents (bit rate and resolution information) of degradation etc. are added if needed A preview license is generated and processing progresses to Step S73 mentioned later.

[0151] A license table is shown in drawing 18. The address information which shows the recording position where license ID of a license and each preview license is usually recorded and the license [ / in the license information database 12 ] is recorded if needed is recorded on the license table for every content ID.

[0152] When it is judged in Step S65 that received data are not preview license acquisition request information received data Usually since it is license acquisition request information in Step S69 the control section 41 transmits the directions about accounting to the personal computer 1 and the settling server 5 which are usually license request origin via I/O interface 42 and the Internet 2.

[0153] In Step S70 the control section 41 judges whether whether the issue request of the usual license of the content ID specified from the settling server 5 to

corresponding user ID being advanced and a user ended accounting with the settling server 5 correctly.

[0154]In Step S70when it is judged that the issue request of a license is not usually advanced from the settling server 5processing progresses to Step S78 mentioned later.

[0155]In Step S70when it is judged that the issue request of a license is usually advanced from the settling server 5in Step S71the same processing as Step S67 is performed.

[0156]In Step S72the control section 41 refers to the license table of the license information database 12 based on the content ID of which the license was usually requiredThe license key for ordinary reproduction corresponding to the demanded contents is searchedUser Information containing the user ID of the user who transmitted license acquisition request information at least is generatedand the usual license which adds and publishes limitation informationsuch as reproduction frequency and a copy guardetc. is generated if needed.

[0157]After the end of processing of Step S68or the end of processing of Step S72in Step S73the control section 41 searches and reads the public key of the user of license request origin from the user registration database 11and supplies it to encryption and the decoding processing section 44.

[0158]the license (the preview license generated in Step S68 — or) which generated the control section 41 to encryption and the decoding processing section 44 in Step S74 It is made to encipher by a corresponding user's public key which was generated in Step S72 and which usually supplied the license and was searched in Step S73.

[0159]The control section 41 makes an electronic signature perform in Step S75 with the secret key for the signature of the license server 3 which controls encryption and the decoding processing section 44and is recorded on the enciphered license by the secret key Records Department 51.

[0160]In Step S76the control section 41 refers to a user's e-mail address registered into the user registration management table of the user registration database 11It is enciphered and the license to which the electronic signature was performed is transmitted to the personal computer 1 of a requiring agency via I/O interface 42 and the Internet 2 (data shown in [ of the inside h of the figure of drawing 13or drawing 14 / n ] a figure).

[0161]In Step S77the control section 41 updates the license issue table of the license information database 12and processing is ended.

[0162]A license issue table is shown in drawing 19. The user ID which published the licensethe content ID which published the licenseand the license status which shows the kind of published license are registered into a license issue table.

[0163]Transmitting [ the received data ] origin in Step S63In [ when it is judged that it is not a user's personal computer 1 registered ] Step S66when it is judged that the conditions for preview license issue are not fulfilledWhen it is judged in Step S70 that



the issue request of a license is not usually advanced from the settling server 5 in Step S78 the control section 41 While displaying an error message on the indicator which is not illustrated and notifying generating of an error to the administrator of the license server 3 If needed via I/O interface 42 and the Internet 2 an error message is also replied to the personal computer 1 and processing is ended.

[0164] Since it licenses [ preview ] or a license is usually transmitted to the personal computer 1 which a user holds from the license server 3 by the processing explained above a user It becomes possible to decode the contents data received from the contents server 4 or other personal computers and to reproduce.

[0165] And contents are in the state where User Information was attached and are delivered and received by the personal computer 1. Since it is enciphered by the public key of the license server 3 User Information is made as [ read / only the license server 3 ]. That is when User Information containing user ID etc. is peer-to-peer with contents is delivered and received and is monitored by the malicious third party it can prevent being abused.

[0166] User Information is included in license acquisition request information and is transmitted to the license server 3 from the personal computer 1. The personal computer 1 overwrites User Information attached to contents using User Information included in a license. Since the license server 3 updates the tracing information table which used and explained drawing 17 and the license issue table explained using drawing 19 based on User Information included in license acquisition request information Processing of the tracing information analysis part 45 explained using drawing 4 enables it to carry out tracing of the contents data flow.

[0167] As opposed to the user (distributing agency user) who was peer-to-peer to other users and distributed contents to them based on the tracing information table which the tracing information analysis part 45 explained using drawing 17 for example For example the point etc. can be published and service of sending a present on a fixed point or usually discounting a pointed fee at the time of license purchase can be provided.

[0168] By whether the user of the distribution destination usually demanded the license or the preview license was required. After it changes the point to publish or he demands a preview license it becomes possible by usually requiring a license to remove the case where he becomes a distributing agency user from point issue etc.

[0169] To it in addition the tracing information analysis part 45 It becomes [ whether a user's taste the distribution capability of contents or the method of a preview is exact and ] possible to analyze in detail based on the tracing information table explained using drawing 17 and the license issue table explained using drawing 19.

[0170] For example. [ whether contents which usually have few demands of a license to the number of demands of a preview license are unattractive contents for a user and ] Or it may say that the method of a preview is not good (for example degradation is strong and the merit of contents is not transmitted [ whose a

reproduction part is not exact ] easily).

[0171]From itwhen the distributing agency user ID of a license is its own user ID usuallythe user is usually demanding the license after a preview license request. In such a caseit is possible that the method of a preview is exact. When the distributing agency user ID of a license is not its own user ID usuallythe userSince the license is usually demandedwithout requiring a preview licenseit is thought that corresponding contents are a very attractive title or an artist for a userand are what wishes to purchase even when he has no preview.

[0172]The user who transmits many license requests to the contents from which distributing agency user ID serves as the contents server 4 checks briskly the website etc. which the contents server 4 exhibitsand can say that he is a user who downloads many contents.

[0173]When distribution former user ID and distribution destination user ID are the same user ID repeatedlyto a license request usually the contentsSince I hear that repetition reproduction is done by the same user as for more than the prescribed number of 1 license and it isit can be said that the degree of satisfaction of contents is very high.

[0174]Since the user who distributes a certain contents to many of other users can think that the friend etc. have been widely recommended since corresponding contents are pleasingit also becomes possible from the distribution situation of contents to guess a user's taste.

[0175]Although it can say that the user mostly registered as a distributing agency user is positive to distribution of contents in a tracing information tableFor examplein [ attach / many user ID to the license acquisition request information from other users of the same contents of the user who is not demanding the usual license of a certain contents / namely ] a tracing information tableWhen mostly registered as a distributing agency usera corresponding userAs a result of previewingeven if he is a case where it is seldom pleasingit turns out that many are distributed to the user who is likely to be pleased with the contentsnamelyit is going to spread contents very positively.

[0176]The user usually mostly registered as a distributing agency user to a license in the tracing information tableOr when distributing agency user ID and distribution destination user ID are usually the same to a licenseThe user mostly registered as a distributing agency user at the time of the preview license request of the contents distributes contents exactly to other usersand the sales of contentsi.e.contribute to improvement in the number of demands of usually a licenseare known.

[0177]The tracing information analysis part 45 can analyze still more various information based on the data registered into the tracing information table and the license issue table besides the contents mentioned above.

[0178]Since User Information used as the basis of tracing information is transmitted to the license server 3 whenever a license request is performed from a user as

explained aboveA contents distribution service entrepreneur is issue of the pointetc. being able to be [ issue ] peer-to-peer and being able to provide promptly the service to the user who distributed contents to other users. Since the volition of the user who tries to distribute contents further increases by thisit becomes possible to promote circulation of contents.

[0179]In a user's personal computer 1 here to license acquisition request information. Its own User Information attached to the processing in which User Information attached to contents is includedand the received licenseThe processing which overwrites User Information attached to contents is the same processingeven if the license to demand is a preview license and it is usually a license. That isalthough there are two kinds of licensesit can be said that processing of the personal computer 1 is very easy.

[0180]That and user ID was attached in the license server 3It is registered by that license status which is preview license acquisition request informationor is usually license acquisition request informationand with content ID. The user ID of the distribution origin of the contents contained in attached User Information and the user ID of transmitting [ license acquisition request information ] origini.e.the user ID of the distribution destination of contentsare registered into a tracing information table. And it is made as [ register / into a license issue table / the user IDthe content IDand the license status of transmitting / license acquisition request information / origin ] at the time of license issue.

[0181]And for examplethe contents distribution service entrepreneur who manages the license issue server 3From the information registered into the tracing information table and the license issue table. Since very detailed information can be acquired about the distribution channel of contentsthe degree of satisfaction of contentsthe effect of a previewa user's tasteor the contents distribution capability of user eachThese information can be utilizedsale of contents can be promoted and customer satisfaction can be improved.

[0182]If it puts in another waywhen transmitting license acquisition request information to the license server 3 in a user's personal computer 1User Information attached to the contents data which comes to hand in a different course from a license is transmittedAnd by performing very easy processing in which the user ID attached to contents data is overwritten by its own user ID attached to the received licenseThe contents distribution service entrepreneur who manages the license server 3 can acquire very detailed information about the distribution channel of contentsthe degree of satisfaction of contentsthe effect of a previewa user's tasteor the contents distribution capability of user each.

[0183]Since according to this invention the user ID of the distributing agency user of contents is registered not only when a license is usually requiredbut when a preview license is requiredTracing of contents is possible when contents are not purchased (a license is not usually required).

[0184]In the personal computer 1 which the user uses according to the processing explained aboveAlthough license acquisition request information is transmitted to the license server 3 and explained as what overwrites User Information indicated in the field attached to the contents corresponding to the case where a license is received by User Information included in the licenseFor examplein [ the license server 3 does not attach User Information to a licenseand ] each personal computer 1Its own user ID is enciphered by the public key of the license server 3User Information is createdand it may be made to overwrite the field attached to contents.

[0185]In that caseas the license which comprises license statusa license keyand limitation information was mentioned aboveit enciphers by a user's public keyand the control section 41 of the license server 3 signs with the secret key for its signatureand transmits to the personal computer 1.

[0186]The control section 61 of the personal computer 1 generates User Information which contains at least what enciphered its own user ID by the public key of the license server 3 saved in the memory 63. And when license acquisition request information is transmittedor when a license is receivedenciphered User Information is overwritten in the field attached to corresponding contents. And it is peer-to-peer and the contents data in which User Information is attached to the personal computer which other users hold is distributed.

[0187]And to the license acquisition request information which the personal computer 1 which received this contents data transmits to the license server 3. Since User Information enciphered by the public key of the license server 3 is attachedthe control section 41 of the license server 3 can control encryption and the decoding processing section 44can decode User Information attached using the secret key of the license server 3and can acquire tracing information.

[0188]Although the pair of the public key and secret key which are used for the data encryption and decoding which a user's personal computer 1 and license server 3 deliver and receive hereand the pair of the public key and secret key which are used for an electronic signature were explained as a respectively different thingIt may be made for the pair of the key a data encryption and the object for decodingand for electronic signatures to use the same thing.

[0189]Record here the contents which the user downloadedin order to decode and reproduce using a license keyare explaining as what uses the personal computer 1but. For examplevariety-of-information processing terminalssuch as a portable telephone set and PDA (Personal Digital Assistant)CD (Compact Disk)DVD (Digital Versatile Disk)Or also in the recording and reproducing device etc. which can play the contents data currently recorded on recording mediasuch as a hard disk with which storage devicesuch as MD (Mini-Disk) (trademark)or an inside was equippedcan be adapted of this invention.

[0190]A series of processings mentioned above can also be performed with software. The computer by which the program from which the software constitutes the

software is included in hardware for exclusive use Or it is installed in the personal computer etc. which can perform various kinds of functions for example are general-purpose etc. from a recording medium by installing various kinds of programs.

[0191]. As shown in drawing 3 this recording medium is distributed apart from a computer in order to provide a user with a program. The magnetic disk 31 (a flexible disk is included) with which the program is recorded the optical disc 32 (CD-ROM (Compact Disk-Read Only Memory).) DVD (Digital Versatile Disk) is included — it is constituted by the package media etc. which consist of the magneto-optical disc 33 (MD (Mini-Disk) (trademark) is included) or the semiconductor memory 34.

[0192] In this Description even if the processing serially performed in accordance with an order that the step which describes the program recorded on a recording medium was indicated is not of course necessarily processed serially it also includes a parallel target or the processing performed individually.

[0193] In this Description a system expresses the whole device constituted by two or more devices.

[0194]

[Effect of the Invention] According to the 1st information processor of this invention an information processing method and the program. The 1st information that acquires contents and is attached to contents the 2nd information for specifying contents And the 4th information including the 3rd information that can specify itself is generated The 5th information required in order to transmit the 4th generated information and to reproduce contents is received Since the 6th information attached to the 5th information is extracted and the 6th extracted information was attached to contents instead of the 1st information attached to contents While receiving the so-called supply of the license for reproducing contents the information for carrying out tracing of the information about circulation of contents can be transmitted to the supplier of a license.

[0195] According to the 2nd information processor of this invention an information processing method and the program. The 1st information that acquires contents and is attached to contents the 2nd information for specifying contents And the 4th information including the 3rd information that can specify itself is generated The 5th information required in order to transmit the 4th generated information and to reproduce contents is received Since the 6th information that can specify itself is enciphered by the public key of the transmission destination of the 4th information and the 6th enciphered information was attached to contents instead of the 1st information attached to contents While receiving the so-called supply of the license for reproducing contents the information for carrying out tracing of the information about circulation of contents can be transmitted to the supplier of a license.

[0196] According to the 3rd information processor of this invention an information processing method and the program. The 1st information peculiar to contents that it is used in order to reproduce contents is recorded The 2nd information attached to

contents from other information processors which hold contentsThe 5th information including the 3rd information for specifying contents and the 4th information for specifying other information processors is receivedThe 1st information corresponding to the contents specified using the 3rd information among the 1st information currently recorded is extractedThe 6th information that includes at least the information which specifies other information processors is generatedSince the 7th information that includes the 6th generated information and the 1st extracted information at least is generated and the 7th generated information was transmitted to other information processors specified using the 4th informationThe contents distribution service entrepreneur who supplies what is called a license for reproducing contents to a userIt becomes possible to acquire the tray sink information for analyzing about the distribution channel of contents,the degree of satisfaction of contents,the effect of a preview,a user's taste or the contents distribution capability of user each.

[0197]Since the 5th generated information was transmitted to the 1st information processor specified using the 3rd information,a userWhile receiving the so-called supply of the license for reproducing contentsThe contents distribution service entrepreneur who can transmit the information for carrying out tracing of the information about circulation of contents to the supplier of a licenseand supplies a licenseIt becomes possible to acquire the tray sink information for analyzing about the distribution channel of contents,the degree of satisfaction of contents,the effect of a preview,a user's taste or the contents distribution capability of user each.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a network composition figure used in order to provide the contents distribution service which was adapted in this invention.

[Drawing 2]It is a figure for explaining the contents management table registered into the contents database.

[Drawing 3]It is a block diagram for explaining the composition of a personal computer.

[Drawing 4]It is a functional block diagram for explaining the function of a license server.

[Drawing 5]It is a flow chart for explaining user registration processing.

[Drawing 6]It is a figure for explaining a user registration management table.

[Drawing 7]It is a functional block diagram for explaining the function of the personal computer which a registered user holds.

[Drawing 8]It is a flow chart for explaining processing of a personal computer.

[Drawing 9]It is a flow chart for explaining processing of a personal computer.

[Drawing 10]It is a figure for explaining flowing into a license and contents,a signature,a

code and User Information.

[Drawing 11] It is a figure for explaining a contents management table.

[Drawing 12] It is a figure for explaining flowing into a license and contents a signature a code and User Information.

[Drawing 13] It is a figure for explaining flowing into a license and contents a signature a code and User Information.

[Drawing 14] It is a figure for explaining flowing into a license and contents a signature a code and User Information.

[Drawing 15] It is a flow chart for explaining processing of a license server.

[Drawing 16] It is a flow chart for explaining processing of a license server.

[Drawing 17] It is a figure for explaining a tracing information table.

[Drawing 18] It is a figure for explaining a license table.

[Drawing 19] It is a figure for explaining a license issue table.

[Description of Notations]

1 A personal computer and 2 The Internet Three license servers and 4 A contents server 5 settling servers and 11 user-registration database 12 A license information database and 13. A contents database and 21 CPU 24 An input part and 27 An outputting part and 26 RAM 30 network interfaces and 41. A control section and 42 I/O interfaces 43 A memory and 44 Encryption and a decoding processing section 45 A tracing data analysis part and 51 [ Encryption and a decoding processing section and 65 / A regeneration part and 71 / The secret key Records Department 72 indicators and 73 / Loudspeaker ] The secret key Records Department and 61 A control section 62 I/O interfaces and 63 A memory and 64

---